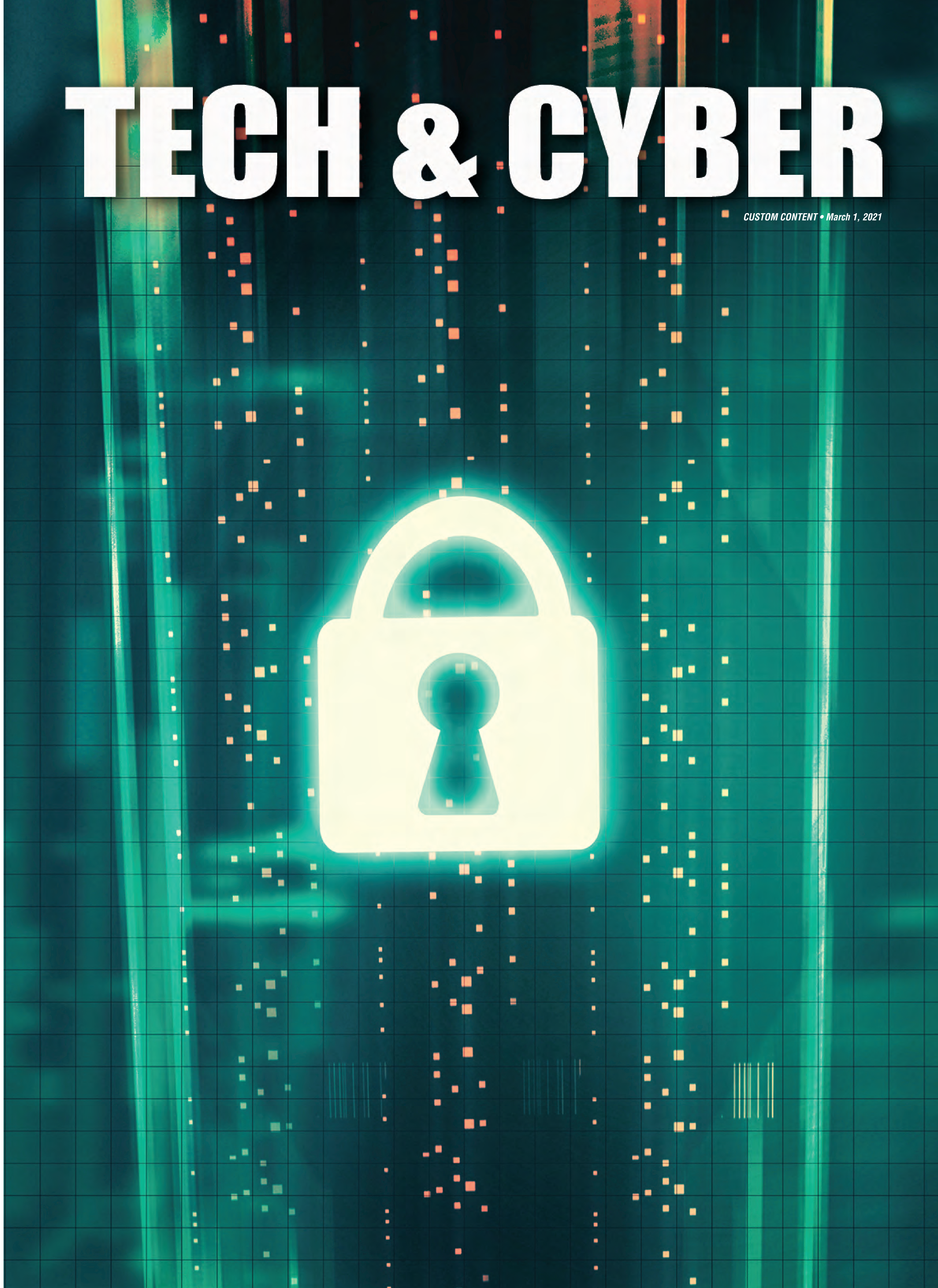
# TECH & CYBER

*CUSTOM CONTENT • March 1, 2021*



# U.S. Immigration Under The New Administration - Impact for Tech & Cyber Security

Just a month into Biden's presidency and the new Administration has unraveled several policies set in place under President Trump's Administration which made it more challenging for US employers to hire professional foreign workers. On January 25, 2021, President Biden revoked President Trump's "Buy American, Hire American" (BAHA) policy, which ultimately led to increased scrutiny and denials of the most common work visas, especially H-1B and L-1 visa categories. The revocation of BAHA is likely to create a more favorable business immigration climate for employers seeking to hire hard to find, professional talent, in the low unemployment fields of high tech and cybersecurity.

Tech and cybersecurity companies are also sure to welcome the United States Citizenship and Immigration Service's (USCIS) recent rescission of a 2017 memo which took the position that computer programmer occupations were no longer presumed to qualify as H-1B specialty occupations. The rescission of this memo means H-1B visa petitions for computer programmers are less likely to be challenged by USCIS.

Miller

Wexler

The most significant immigration action to date has been a comprehensive immigration reform bill, which President Biden submitted to congress on his first day in office. The bill includes several provisions which would impact tech and cyber security employers, including a reduction of lengthy green card wait times for employer-sponsored professionals, and prioritization of green cards for Ph.D. professionals in the STEM fields. While these provisions would ameliorate some issues that have plagued U.S. business immigration for decades, the extensive bill is not expected to receive the votes necessary to be enacted by Congress.

President Biden's numerous immediate actions to unravel Trump-era restrictive immigration policies evidences the new Administration's stance towards immigration reform. Whether the Biden Administration can cure some of the US immigration system's larger systemic issues may ultimately depend on his ability to get congressional support for more targeted, piecemeal reform and not overly broad comprehensive bills.

Mitch Wexler is the Managing Partner of Fragomen's Irvine office. Fragomen, with 50 offices and 4,500 employees worldwide, is the leading business immigration law firm in the world. Mitch can be contacted at mwexler@fragomen.com

Blake Miller is a Partner with Fragomen's Irvine office. Blake can be contacted at bmiller@fragomen.com

C3 TECH

# C3 Tech Achieves Platinum Partner Status with Datto

Santa Ana, CA 2/19/2021 – C3 Tech today announced it has achieved the exclusive Platinum partner status with Datto, the leading global provider of cloud-based software and technology solutions purpose-built for delivery by managed service providers (MSPs). Datto's Platinum status represents the top 10 percent of the company's partners, worldwide.

Tricia Sanchez

C3 Tech has exceeded high standards of performance to qualify for Platinum status within Datto's Global Partner Program. Platinum status includes many exclusive programs and benefits designed to support further enablement and business growth.

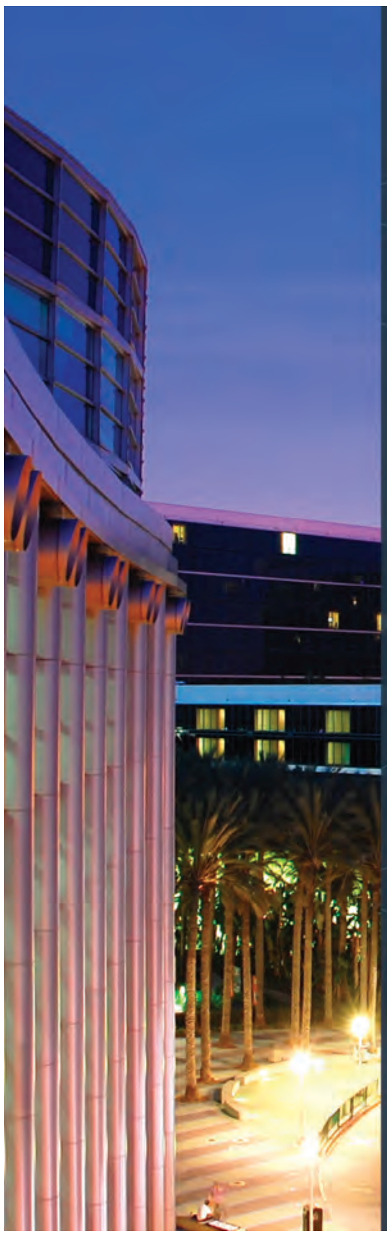
C3 Tech has been a Datto Partner for many years catering to businesses that need IT Support and Infrastructure. With Datto as their partner, they are able to provide Remote Desktop Support, Data Backup, Firewall Protection, Ransomware Detection and Spam Filtering.

"It's an honor to be part of an elite group of successful Datto partners. The company has played an integral role in our ability to hit our sales and marketing objectives." – Tricia Sanchez

"We are thrilled that C3 Tech has reached Platinum Partner Status," said Rob Rae, senior vice president of business development, Datto. "It's been fantastic to see C3 Tech leveraging our training, support and marketing resources to take their business to the next level. We look forward to more success in 2021 as we continue to roll out new partner services."

C3 Tech is and IT Service and Office Technology Company located in Santa Ana, California. A leading organization for over 25 years providing full service solutions with best in class partners and products that fit any technology need to evolve their business.

From now until the end of summer, C3 Tech is offering free data backup hardware and security package for $17 a month per device. Mention #C3TechPlatinum when calling in or email **at info@c3tech.com**.



Maschoff Brennan
INTELLECTUAL PROPERTY AND COMPLEX LITIGATION

# That Invention is Not Obvious! Hindsight Is Worse Than You Think

A recent newspaper article about the inventor of the traffic light observed: “It seems so obvious now. But then that’s the thing about inventions. They’re always plain to see in hindsight.” As the saying goes, “hindsight is 20/20.” The U.S. Patent Office, however, is often dismissive of this basic insight.

In my experience filing hundreds of patent applications, the Patent Office is frequently dismissive of the effect hindsight has on its determination of obviousness for a claim of a patent or patent application. This should be no surprise. Examiners are simply following the guidance provided by the MPEP — the Patent Office official manual establishing ground rules for granting or denying an application. The MPEP is sparing in its guidance on avoiding hindsight, stating:“[h]owever, ‘[a]ny judgment on obviousness is in a sense necessarily a reconstruction based on hindsight reasoning, but so long as it takes into account only knowledge which was within the level of ordinary skill in the art at the time the claimed invention was made and does not include knowledge gleaned only from applicant’s disclosure, such a reconstruction is proper.’” This terse statement dramatically downplays the effect hindsight has on the obviousness analysis the Patent Office performs. The general belief seems to be that so long as an examiner is aware that he or she should be able to avoid hindsight, that awareness of the principle suffices, without more, to avoid the use of hindsight in evaluating whether an invention would have been obvious.

This Patent Office view, however, is starkly inconsistent with both common sense and the well documented understanding that people are generally incapable of avoiding hindsight even when overtly attempting to do so. For example, in an oft-cited study, subjects were given a scenario and asked to assign the probability to four different potential outcomes. In one group, no actual outcome was provided to the subjects. In another four groups, subjects were told that one of the four outcomes was the “true” outcome, but were told to respond “as they would have had they not known the outcome.” This study is widely recognized for its methodological simplicity and rigor in demonstrating a principle directly at odds with the MPEP statement. What it shows is that, in 13 of 16 cases, the mean probability of the “true” outcome was substantially higher for the group that was told to ignore the “true” outcome when responding. On average, the probability of an event increased from an average 25% in the group that had no knowledge of the outcome, to an average of 34% in the group that was told to ignore what it knew. This suggests that relying on forethought to avoid hindsight results in significant error.

Applying the statistical adjustment for forethought to the Board’s decision, one can make the following observation. If the Board or an Examiner, applying the prevailing preponderance of the evidence standard for determining obviousness, believes that a claim is 51% likely to be obvious, the variance reflected by the study described above suggests that the probability that the claims are obvious is in fact about 18% lower, or 33%. It follows that for most cases that seem to be close, the Patent Office is usually wrong when it determines that the claims are obvious. Similarly, for a truly close case, the Board or Examiner, failing to adjust for the bias of hindsight, would probably believe that the likelihood of obviousness is about 68%. With the unavoidable effects of hindsight, perhaps the clear and convincing standard used by the courts in reality yields a result that in fact is closer to the preponderance of the evidence standard that the MPEP intends to be the correct basis for determining whether an application is obviousness. This observation itself seems obvious.

Brent Johnson, Ph.D. is a shareholder in Maschoff Brennan’s Orange County office. He is focused on patent prosecution, BPAI post grant proceedings, IP due diligence, and client counseling, particularly in the areas of pharmaceutical and other chemistry-related technologies.

# A Q&A with Entisys360's Brad Bussie

With ever-emerging threats, continuous introduction of new regulations, and a sea of cybersecurity products, managing a cyber program can be challenging. Entisys360's Advyz Cyber Risk Services division focuses on cybersecurity consulting with an emphasis on enabling stakeholders to solve complex business challenges. We are product vendor agnostic, which allows us to serve our clients as true trusted advisors. Our approach provides us the necessary tools to work closely with our clients to ensure that their organizations have the right people, processes, and technologies in place to navigate the ever expanding world of cyber threats.

One of the areas of cybersecurity that is making headlines today is 'zero trust.' We sat down with Brad Bussie, Vice President, Advyz Cyber Risk Services, to learn more about this concept and what it means for customers.

**1) Ever since an analyst at Forrester Research coined the term 'zero trust' a decade ago, there has been growing interest in and adoption of the zero trust model for security. What should customers know when it comes to implementing and achieving zero trust?**

It's true that the concept of zero trust remains something that the market is very interested in. When we are talking to a client or potential client about zero trust, while many understand it within the context of the Forrester model, they don't clearly understand the benefits, or what the term means within the context of their business. The old way of looking at zero trust, is to trust nothing. The challenge is that this approach to zero trust doesn't scale. In fact, it prevents organizations from performing tasks outside of what a particular technology is intended to do. Organizations need to take a step back and first determine what it is they are trying to protect in the first place. Here at Advyz, we are working with our customers to help them understand that zero trust isn't a product or solution, instead it is a loose framework of processes that can be tailored based on the specific needs of the organization.

**2) What is the size of the market right now for zero trust?**

According to MarketsandMarkets Research, the global **zero trust** security **market size** is estimated to grow from USD $15.617 million in 2019 to USD $38.631 million by 2024, at a Compound Annual Growth Rate (CAGR) of 19.9% from 2019 to 2024.

**3) We hear the term SASE a lot these days. What does that have to do with zero trust?**

SASE, or secure access service edge, is a hot term right now in the cybersecurity space. It is driving many of the conversations we have with our clients, and definitely falls into the overarching message around zero trust. In fact, it can be a gateway to creating a zero trust framework for many organizations, as it is where they are finding budget. The reality is that the C-suite is more likely to spend money on solutions that will protect data, applications, and infrastructure security as opposed to frameworks. Entisys360 helps our clients by enabling them to define what it is they are ultimately trying to protect. Success won't come from "boiling the ocean", because it is impossible, and impractical, to protect everything to the same degree. We encourage our clients to leverage the zero trust model to look at what's most important and to apply zero trust principals throughout the environment.

**4) Can you share an example of where micro-segmentation has worked?**

One example of successful micro-segmentation is with an access control engine. This is an area where many organizations struggle because they don't understand the flow of data in and out of the organization. The point of access control is to provide users with only the access they need to the data, applications, and infrastructure to do their jobs. Once an organization implements an access control engine, they often find that they already have what they need (i.e. firewalls, proxy servers, etc.) to grant users access to only the right resources. As such, in many cases they don't need to purchase additional products or solutions to increase visibility and properly segment traffic.

**5) What are some of the most important steps to consider as part of the zero trust model?**

First and foremost, it is important to remember that you can't manage what you don't measure. Step one when implementing the zero trust framework is to identify and map the relationship between the organization's data, applications, and networks. Next, you have to identify what benefits the users and other key stakeholders within the organization gain by participating in the zero trust program. Education is key to helping the organization understand how to reduce risk and promote security in all they do.

**6) What are the outcomes I should expect when implementing the zero trust model?**

When an organization adopts the zero trust model it will experience the following benefits:

- A more secure network
- Improved focus across the organization on protecting data, application and infrastructure
- Enhanced protection against existing and evolving threats – i.e., zero day
- Reduced impact from breaches
- Improved compliance and visibility
- Potential cost savings in people, process and technology required to protect the organization due to the simplified environment.

Last, but not least, the organization will finally gain a full understanding of the technology it is using and how it should be applied in order to promote a secure infrastructure environment.

**Brad Bussie**

Brad Bussie is an award-winning information security professional with experience in cybersecurity, identity/access management, vulnerability management, governance, risk, and compliance. Over the last 16 years, Brad has served as a security strategist, industry thought leader and author. After earning an MBA in information security management, he was also awarded premier certifications from multiple vendors in the cybersecurity space, including the CISSP from ISC2.

Since joining Entisys360, Brad has focused on building the Advyz Cyber Risk Services division by bringing people, processes, and technology together to help organizations solve their most pressing cybersecurity and business challenges.

**About Entisys360**

Entisys360 is an award-winning IT consultancy specializing in end-user computing, cloud, automation, software defined infrastructure, and cybersecurity. For nearly three decades, Entisys360 has helped government, education and healthcare organizations achieve their business goals through product advisory services, technical consulting, and systems integration.

# Security and Cyber Risk Services

Advyz
CYBER RISK SERVICES
*a division of* **Entisys360**

The Advyz Cyber Risk Services team partners with clients to ensure that your organization is prepared and has the tools and technologies in place to protect your data, applications and infrastructure in the event of a data breach or other cybersecurity incident.

## Our Team

Our team comprises highly skilled and experienced cybersecurity professionals.

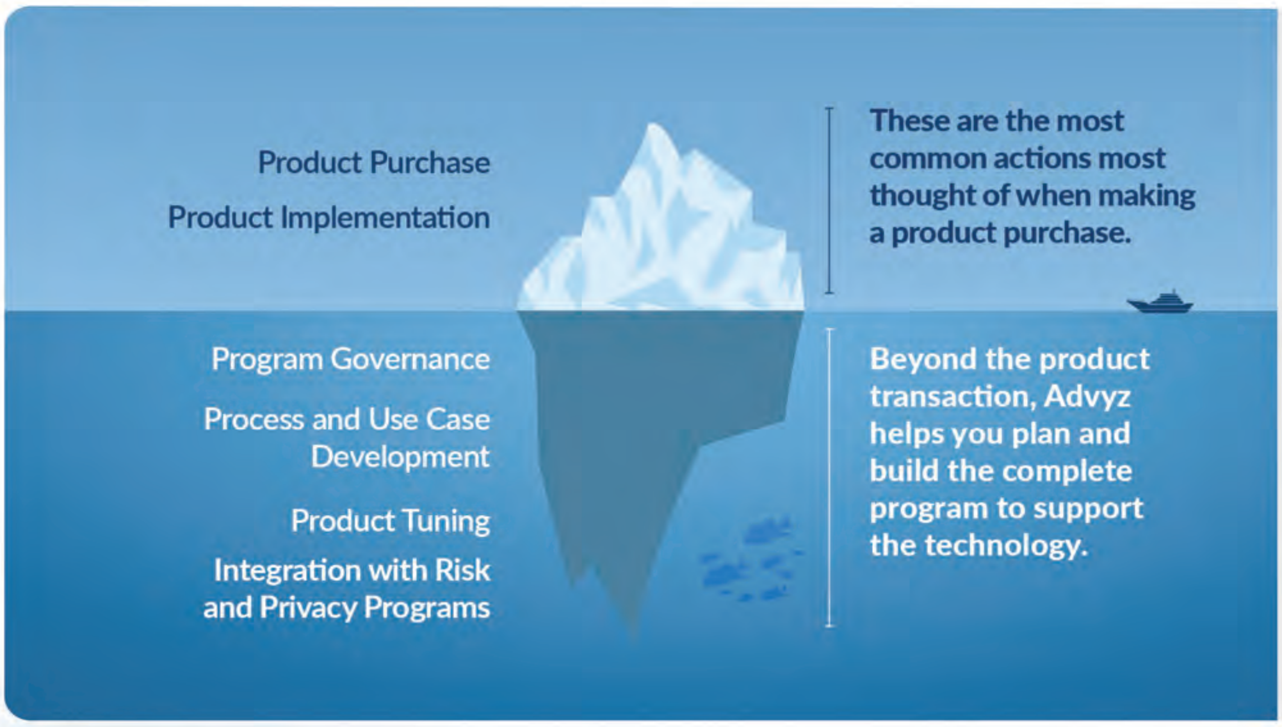
77%

**Certified Information Systems Security Professional (CISSP)**

62%

**Chief Information Security Officers (CISO)**

**ADDITIONAL CERTIFICATIONS -** PCI QSA,CISM, CISA, CRISC, GIAC GWEB/GWAPT/GMOB, PMP, CPT, ENCE, IAM, and dozens of vendor certifications



Product Purchase

Product Implementation

These are the most common actions most thought of when making a product purchase.

Program Governance

Process and Use Case Development

Product Tuning

Integration with Risk and Privacy Programs

**Beyond the product transaction, Advyz helps you plan and build the complete program to support the technology.**

## Our Approach

We bring leading cyber security products to your organization through a consultative approach. Our focus is enabling program goals by aligning people and process with technology. We are your advocate and advisor to help you navigate the vast universe of security products.

## Our Solutions

We strive to help you do more with what you have, making the most of investments in your people and technology.

- **STRATEGY AND RISK MANAGEMENT**
- **ATTACK SURFACE MANAGEMENT**
- **DETECTION AND RESPONSE**
- **IDENTITY**
- **PRIVACY**

## Contact Us

**To speak with a consultant, contact us at advyz@entisys360.com, or learn more at advyz.entisys360.com.**